

EXHIBIT A

BakerHostetler

Baker&Hostetler LLP

312 Walnut Street
Suite 3200
Cincinnati, OH 45202-4074

T 513.929.3400
F 513.929.0303
www.bakerlaw.com

Patrick H. Haggerty
direct dial: 513.929.3412
phaggerty@bakerlaw.com

August 30, 2023

FOIA CONFIDENTIAL TREATMENT REQUESTED

VIA E-MAIL (MARISA.SMITH@HHS.GOV)

Marisa M. Smith, PhD
Regional Manager
U.S. Department of Health and Human Services
Office for Civil Rights
1301 Young Street, Suite 106
Dallas, TX 75202

*Re: Texas Children's Hospital
OCR Transaction Number: 23-529752*

Dear Dr. Smith:

As you know, Texas Children's Hospital ("TCH") has engaged our law firm to assist in the investigation regarding the U.S. Department of Health and Human Services ("HHS"), Office for Civil Rights ("OCR") second request for information, dated August 8, 2023 ("Request"), pursuant to the Federal Standards for Privacy of Individually Identifiable Health Information and/or the Security Standards for the Protection of Electronic Health Information (45 C.F.R. Parts 160 and 164, Subparts A, C, and E, the Privacy and Security Rules), and the Breach Notification Rule Subpart D – Notification in Case of Breach of Unsecured Protected Health Information (45 C.F.R. §§ 164.400-164.414).¹

Certain information being provided in response to OCR's Request constitutes proprietary and confidential information that is exempt from a Freedom of Information Act request, and TCH respectfully requests that OCR take all available steps to prevent this information from being produced to third parties and asserts all available protections regarding this information so that it will not be released without TCH's express written authorization. Further, as you know, the FBI and HHS OIG have ongoing investigations into the Physician's potential criminal activity. Thus, the disclosure of information in this response and documents produced with it to the public could disrupt an ongoing federal law enforcement investigation and, to the extent the Physician was not

¹ Our response and exhibit numbers correspond with the number set forth in the Request.

August 30, 2023

Page 2

involved, irreparably damage his reputation. For this additional reason, TCH requests and expects HHS OCR not to disclose this response and documents produced with it in response to any requests. TCH is available to discuss any questions you may have with respect to the request for confidentiality.

On behalf of TCH, BakerHostetler is producing documents responsive to the OCR's Data Request in electronic format. The total page count for this document production is 258 pages (Bates numbers TCH001331-TCH001588).

As detailed in our prior response and this response, TCH has a culture of compliance and transparency regarding information security. This is reflected in the numerous policies and procedures and controls in place. It should not be lost on HHS OCR that the evidence indicates that a Physician, who has an ethical duty to protect patients, used his legitimate access to protected health information (PHI) to acquire and disclose certain PHI to a conservative activist who subsequently published an online article that included redacted schedules. No set of controls will prevent such malicious and intentional acts.

Requests

1. **Does Texas Children's "Managing User Access to Texas Children's Information System" policy control the process whereby medical students, interns, residents, and non-employee physicians are granted approval to access Texas Children's electronic protected health information (ePHI), including its electronic medical record (EMR)? If not, please explain and provide the applicable policies and procedures.**

Response: Yes, the Managing User Access to Texas Children's Information System Policy and Standard applies to medical students, interns, residents, and non-employee physicians.

2. **Please provide a detailed description of how the "Managing User Access to Texas Children's Information System" (or equivalent policy) for medical students, interns, residents, and non-employee physicians is implemented.**

Response: This is detailed in the standard that was previously produced as Exhibit 8.02. Exhibit 2.01 details access management for the Epic application, TCH's EMR. The Epic Provisioning Procedure, which was previously produced as Exhibit 8.07, details activating, deactivating, and reactivating accounts including those for medical students, interns, residents and non-employee physicians. Exhibit 2.02 details the creation of Epic security templates. TCH's Data Access and Use Procedure is produced as Exhibit 2.03.

All non-employees requiring access to Texas Children's information or information assets must have a Texas Children's manager based on Texas Children's Level of Authority who is responsible for ensuring that the access rights and privileges to be granted are based upon the minimum amount of information needed to complete tasks or job responsibilities.

August 30, 2023
Page 3

Upon approval by the manager or above, non-TCH employees such as medical students, interns, residents, and non-employee physicians are assigned a unique Active Directory user account before allowing them to access system components. Standard user access includes User ID, Exchange User Mailbox, personal drive and a default share drive associated with the user's cost center.

For Epic, requests for new access or modification to existing access is submitted through a centralized IT ticketing system, ServiceNow. A copy of the form was previously produced as Exhibit 8.05. The access request is approved by a manager or above. If approved, a ServiceNow ticket is generated and routed to the TCH Information Security Epic Security queue for processing. A copy of a ServiceNow ticket was previously produced as Exhibit 8.06. The Identity Access Management (IAM) analyst logs into Epic and provisions access following the steps in the Epic Provisioning Procedure which was previously produced as Exhibit 8.07. The ServiceNow ticket is then updated, the requestor is notified that access has been granted and the ticket is closed.

3. **Please provide a copy of Texas Children's "Remote User Access Policy" or the equivalent policy, for medical students, interns, residents, and non-employee physicians. If not addressed in the Remote User Access Policy, please provide an explanation and documentation of the process by which students, interns, residents, and non-employee physicians are provided with remote access to Texas Children's information systems containing ePHI.**

Response: A copy of TCH's Remote User Access policy is attached as Exhibit 3.01 which applies to the entire workforce, including medical students, interns, residents, and non-employee physicians.

4. **Are any restrictions applied to medical students, interns, residents, and non-employee physicians who are approved to access Texas Children's ePHI, including its EMR? Please explain and provide any supporting documentation, including documentation pertaining to role-based access, least privilege, and any technical safeguards, if not provided previously.**

Response:

Yes, restrictions are applied to medical students, interns, residents, and non-employee physicians who are approved to access TCH's ePHI, including Epic. For Epic, medical students, interns, residents, and non-employee physicians are assigned a specific template based on their role and least privileges. A copy of the resident template – LINK, RESIDENT INT DL, is attached as Exhibit 4.01. Epic contains restrictions such as requiring a user to re-authenticate to re-activate a terminal or session that has been idle for more than 15 minutes.

August 30, 2023
Page 4

Active Directory accounts that have been inactive for 90 days are disabled by automated provisioning software. Active Directory accounts are automatically deleted after 120 days from the account being disabled.

Multi-factor authentication is in place for remote access.

5. The HHS Office of Inspector General ("OIG") has identified an individual ("Physician") who accessed ePHI maintained by Texas Children's and potentially disclosed that information to City Journal.

a) Please describe the relationship Physician had to Texas Children's, including when the relationship began, what services were provided, whether those services changed over time, etc.

Response:

The Physician was a resident with Baylor College of Medicine ("BCM") from June 24, 2018 until June 23, 2023. General pediatric surgery residents are assigned general pediatric surgery responsibilities. They are responsible for the pre-, intra-, and postoperative care of pediatric general surgery patients. The care ranges from emergency room to the operating room to the ICU. They cover all of the patients of the pediatric general surgery faculty.

The Physician rotated at TCH as follows:

Pediatric General Surgery

- June 2019
- August 2019
- April 2020
- August 10, 2020 through September 19, 2020
- December 10, 2020 through January 18, 2021

Transplant Surgery

- August 2018
- April 10, 2021 through May 20, 2021
- October 8, 2021 through November 23, 2021

Coverage at Pavilion for Women²

² Residents assigned to any of the Baylor St. Luke's Medical Center (BSLMC) general surgery rotations may also treat patients at TCH's Pavilion for Women as the BCM BSLMC general surgery faculty also provide coverage at TCH's Pavilion for Women.

August 30, 2023

Page 5

- December 2018
- January 2019
- May 2019
- June 24, 2020 through August 9, 2020
- October 30, 2020 through December 9, 2020
- January 19, 2021 through February 28, 2021
- June 24, 2022 through August 4, 2022
- December 27, 2022 through January 31, 2023
- April 12, 2023 through June 23, 2023

b) Please provide documentation of Physician's request(s), authorization(s), and approval(s) to obtain access (and remote access) to Texas Children's EMR.

Response:

The Physician's Active Directory account was created on April 11, 2018 with a start date of June 19, 2018. *See Exhibit 5.01.*³ Access was appropriately approved by TCH's Practice Administrator for Pediatric Surgery at the time. The Physician's Active Directory account was automatically disabled on March 19, 2022 because it expired. The Active Directory account was deleted on July 17, 2022, 120 days after the account became disabled. Epic access is tied to Active Directory and, therefore, when the Active Directory account is disabled so is access to Epic.

The Physician's Epic account was created on April 15, 2018 and listed as inactive pending training. *See Exhibit 5.02.* Following training, the Physician's Epic account was updated from inactive to active on June 19, 2018. *See Exhibit 5.03.* The Physician was assigned resident Epic template. *See Exhibit 5.04.* As an additional control, TCH audits Epic access annually. As part of TCH's annual attestation process, on October 26, 2020, the Physician's Epic access was deactivated because the attester did not attest to the Physician requiring access. *See Exhibit 5.05.*

On September 30, 2022, the Physician contacted TCH's Project Analyst for the Department of Pediatric Surgery requesting reactivation of his access because he had more rotations where he would see TCH patients. *See Exhibit 5.06.* Given that the Physician's Active Directory account had been deleted, TCH's Project Analyst put in a request to create a new Active Directory account. *See Exhibit 5.07.* This was approved by TCH's Practice Administrator for Pediatric Surgery who would be responsible for approving pediatric resident access requests. *See Exhibit 5.08.* The Physician's Epic ID was updated to comport with the new Active Directory account on September 30, 2022. *See Exhibit 5.09.*

³ The exhibits in response to this request have been redacted and PHYSICIAN has been added where the Physician's full or partial name or appears.

August 30, 2023
Page 6

TCH's Project Analyst also put in a request for remote access for the Physician. *See Exhibit 5.10.* This was approved by TCH's Practice Administrator for Pediatric Surgery. *See Exhibit 5.11.*

On October 26, 2022, TCH's Project Analyst provided the IAM team with a list of medical students, residents, and fellows who had been approved by their management for Epic access. *See Exhibit 5.12.* The Physician had approved access. The Project Analyst again provided a list of Epic approved medical students, residents, and fellows on March 21, April 13, and May 3, 2023. *See Exhibits 5.13 – 5.15,* respectively. The Physician had approved access.

The Physician's Active Directory account was disabled by automated software due to inactivity on January 11, 2023. *See Exhibit 5.16.* On January 16, 2023, the Physician reached out to the help desk for assistance and was told to contact his manager. *See Exhibit 5.17.* The Physician reached out to TCH's Project Analyst on January 19, 2023 to re-enable his account. *See Exhibit 5.18.* Given the Physician's approved access, the Physician's Active Directory account was re-enabled, but the Physician must login the same day the account is re-enabled, or the account is disabled. The Physician did not login the day the Active Directory account was re-enabled, and the account disabled. *See Exhibit 5.19.*

On or about April 14, 2023, the Physician reached out to TCH's Project Analyst to have his account re-enabled. *See Exhibit 5.20.* Given the Physician's approved access, the account was re-enabled on April 14, but the Physician did not log in that day and the account was disabled. *See Exhibit 5.21.* The Physician's Active Directory account was re-enabled on April 20, 2023, but the Physician did not log in that day and the account was disabled. The Physician's Active Directory account was re-enabled on April 21, 2023 and the Physician logged into the account that day. *See id.*

c) Who authorized Physician's access in and, if different, who was the Physician's sponsor?

Response:

TCH's Practice Administrator for Pediatric Surgery, who was the Physician's manager, authorized the Physician's access.

d) Who approved Physician's access?

Response:

TCH's Practice Administrator for Pediatric Surgery, who was the Physician's manager, approved the Physician's access.

August 30, 2023
Page 7

e) Were any connection time controls, as referenced in the user access policy cited above, applied to Physician's access?

Response:

Yes. Please see response to 5(a) above which details the time controls that operated as intended and in accordance with policy.

f) Please identify the Data Managers and/or the Data Custodians of the information that was impermissibly disclosed by Physician. To what extent were the Data Manager and/or the Data Custodians aware of Physician's access to such data in 2023?

Response:

The information that was impermissibly disclosed came from Epic. Access to Epic is governed through templates which are designed based on job role and least privileges. TCH has an Epic Security Cross Functional Work Group that is responsible for approving new Epic templates and modifying existing templates. The group's charter is produced at Exhibit 5.22. Any changes to existing templates is tracked. This Group ensures that access based on the template is necessary, appropriate, and based on least privileges. Further, TCH has an annual attestation process where the manager must attest that the workforce member requires access to Epic and the template is appropriate based on role.

g) Was Physician's access to Texas Children's EMR in 2023 detected and flagged by Texas Children's security information and event management protocols prior to publication of Texas Children's PHI? If yes, please describe and provide documentation. If not, please explain.

Response:

The Physician had approved and authorized access to TCH's EMR. Accordingly, TCH's security information and event management protocols would not have detected and flagged the Physician's access.

h) If Texas Children's policies and procedures were not followed when Physician was granted (or retained) access to Texas Children's ePHI, please explain and provide documentation of any corrective actions taken.

Response:

TCH's policies and procedures were followed.

Should you have any questions, please do not hesitate to contact me.

August 30, 2023

Page 8

Sincerely,

A handwritten signature in blue ink, appearing to read "Patrick H. Haggerty".

Patrick H. Haggerty
Partner

Enclosures

cc: Melissa Murrah, Vice President & Privacy Officer, Texas Children's Hospital
Tessy Carpenter, Director, Compliance and Privacy Office, Texas Children's
Hospital